# A ROBUST VIDEO WATERMARKING USING SIMULATED BLOCK BASED SPATIAL DOMAIN TECHNIQUE

FARNAZ ARAB

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

DECEMBER 2014

To my beloved husband

To my beloved father and mother

To my beloved sisters and brothers

## ACKNOWLEDGEMENTS

I would like to thank my principal supervisor, Dr. Mohd Shahidan bin Abdullah for his guidance during my research and study. His perpetual energy and enthusiasm in research had motivated me. I would also like to thank my co-supervisor, Assoc. Prof. Dr. Siti Zaiton Mohd Hashim, for her support and encouragement. I especially want to thank Prof. Dr. Azizah Bt Abdul Manaf, and Prof. Dr. Rosalina binti Abdul Salam as my thesis committee members. They read my thesis rigorously and helped me to correct it.

# ABSTRACT

A digital watermark embeds an imperceptible signal into data such as audio, video and images, for different purposes including authentication and tamper detection. Tamper detection techniques for video watermarking play a major role of forensic evidence in court. The existing techniques for concealing information in the multimedia host are mostly based on spatial domain rather than frequency domain. The spatial domain techniques are not as robust as frequency domain techniques. In order to improve the robustness of spatial domain, a watermark can be embedded several times repeatedly. In order for spatial domain techniques to be more efficient, more payload is needed to embed additional information. The additional information would include the redundant watermarks to ensure the achievable robustness and more metadata of pixels to ensure achievable efficiency to detect more attacks. All these required additional information will degrade the imperceptibility. This research focuses on video watermarking, particularly with respect to Audio Video Interleaved (AVI) form of video file format. The block-wise method is used to determine which block exactly altered. A high imperceptible and efficient tamper detection watermarking technique is proposed which embeds in first and second Least Significant Bits (LSB). The proposed technique divides the video stream to 2*2 non-overlapping simulated blocks. Nine common attacks to video have been applied to the proposed technique. An imperceptible and efficient tamper detection technique with a novel method of video segmentation to comprise more pixels watermarked is proposed. Experimental results show the technique is able to detect the attacks with the average of Peak Signal-to-Noise Ratio (PSNR) as 47.87dB. The results illustrate the proposed technique improves imperceptibility and efficiency of tamper detection.

# ABSTRAK

Tera air digital membenamkan isyarat tidak kelihatan ke dalam data seperti audio, video dan imej, untuk tujuan yang berbeza termasuk pengesahan dan pengesanan gangguan. Teknik pengesanan gangguan untuk tera air video memainkan peranan utama sebagai bukti forensik di mahkamah. Teknik sedia ada dalam penyembunyian maklumat hos multimedia adalah kebanyakkannya berdasarkan domain *spatial* berbanding dengan domain frekuensi. Ketahanan teknik domain *spatial* tidak seteguh teknik domain frekuensi. Pendekatan yang paling biasa untuk menyembunyikan maklumat dalam multimedia adalah menggunakan domain *spatial*. Kemantapan dari segi keteguhan, teknik domain *spatial* adalah tidak setinggi berbanding dengan domain frekuensi. Dalam usaha meningkatkan keteguhan domain *spatial*, tera air boleh dibenamkan secara berulang kali. Bagi menjadikan teknik domain *spatial* lebih cekap, lebih muatan diperlukan untuk membenamkan maklumat tambahan. Maklumat sampingan termasuk tambahan tera air adalah dikehendaki untuk memastikan keteguhan dicapai dan bagi memastikan kecekapan boleh diperolehi serta mengesan lebih banyak serangan lebih metadata bagi piksel diperlukan. Semua maklumat tambahan yang dimasukkan ini akan mengurangkan kualiti video. Kajian ini memberi tumpuan kepada tera air video, terutamanya berkaitan dengan format Audio Video (AVI). Kaedah *block-wise* diguna bagi menentukan secara tepat blok yang diubah. Pengesanan gangguan dan ketinggian mutu dengan menggunakan tera air Bit Terkurang Bererti (LSB) pertama dan kedua adalah dicadangkan. Teknik yang dicadangkan akan membahagikan aliran video kepada 2*2 blok simulasi secara tidak bertindih. Sembilan serangan untuk video telah diuji kepada teknik yang dicadangkan. Hasil uji kaji menunjukkan teknik yang dicadangkan mampu mengesan serangan dengan purata Isyarat Puncak Kepada Nisbah Bunyi (PSNR) 47.87dB. Keputusan ini menunjukkan teknik tersebut berjaya menambah baik kualiti dan juga kecekapan pengesanan gangguan.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| AI | - | Artificial Intelligence |
| CD | - | Compact Disc |
| DVD | - | Digital Video Disc |
| DFT | - | Discrete Fourier Transform |
| DCT | - | Discrete Cosine Transform |
| DWT | - | Discrete Wavelet Transform |
| IDWT | - | Inverse Discrete Wavelet Transform |
| DVS | - | Digital Video Surveillance Systems |
| dB | - | Decibel |
| CCTV | - | Closed Circuit Television |
| HAS | - | Human Auditory System |
| HVS | - | Human Visual System |
| LSB | - | Least Significant Bit |
| MSB | | Most Significant Bit |
| RIFF | - | Resource Interchange File Format |
| AVI | - | Audio Video Interleave |
| MPEG | - | Moving Picture Experts Group |
| JPEG | - | Joint Photographic Experts Group |
| RSA | - | Rivest, Shamir, & Adleman (Public Key Encryption Technology) |
| PCA | - | Principal Component Analysis |
| PSNR | - | Peak Signal-to-Noise Ratio |
| NC | - | Normalized Cross-Correlation |
| VW16E | - | Video Watermarking 16 End |
| VW16F | - | Video Watermarking 16 First |
| VW8F | - | Video Watermarking 8 First |

## LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

## 1.1 Overview

A digital watermark is a kind of indication, which is accommodated in the host medium such as digital image, audio, text, software or video. It can be commonly used for ownership protection. Watermarking is a technique of covering digital information in the carrier signal (host). The hidden data is not necessarily related to the content of the host (Chang, Wang, *et al.*, 2011; Junxiao *et al.*, 2011; Liu, 2012). Particularly for video files, in order to solve the problem of unlawful manipulation and dishonest distribution, video watermarking is applied (Liu *et al.*, 2009; Sinha *et al.*, 2011).

Digital Video play a major role of forensic evidence in court (Su *et al.*, 2008; Xu *et al.*, 2010). Hence the video files should be authenticable with ability to detect the tamper, thus a technique like watermarking is applied for the purpose. The watermark must not have any effect on visual information and must not reduce the ability for compromise on the video evidence. Therefore, high imperceptible watermark has responded to the mentioned necessity (Su *et al.*, 2008). Video tamper detection is the challenge of today's researchers in the field of multimedia security (Van Schyndel, 2010).

Although video watermarking has many properties, the main three properties are imperceptibility, robustness and payload or capacity which are closely related to each other for example when the robustness increases, imperceptibility would be decrease and vice versa (Agarwal *et al.*, 2012; Yu *et al.*, 2014). The correct balance

between these conflicting requirements of watermarking should be found for any application and techniques (Agarwal *et al.*, 2012; Ishtiaq *et al.*, 2009).

## 1.2 Background of the Problem

Nowadays cameras in many circumstance has been installed, even these cameras mounted on the streets for fights, drug deals and other improper activities in an environment. The police might see the crime as it was happening or use the video to help in any consequent investigation. Digital multimedia content can easily be duplicated and stored and even without losing fidelity. In Digital Video System (DVS) video file is very vital, because it can be used as a piece of evidence, on the other hand; manipulating the video file by many editing video software in the market is like a piece of cake, so easy and simple with low cost (Sinha *et al.*, 2011).

By growth of communication network, due to the characteristics of digital products such as easy to transform and easy to copy, digital tamper detection has been critical issues which need to be solved (Agarwal *et al.*, 2012). Techniques used for video watermarking tamper detection compared to digital image are stagnant (Agarwal *et al.*, 2012). Ascribable to the natural redundancy between the video frames, proposed techniques for image tamper detection are not appropriate for digital video watermarking which are not presented for attacks including frame dropping, frame inserting, frame shifting and etc. Beside these attacks, techniques are restricted in ability to detect the tamper areas (Sinha *et al.*, 2011).

The tamper detection technique has to be designed to ensure the verification of video content and preventing forgery. Researchers have proposed digital watermarking to verify integrity of content for digital video (Chimanna and Khot, 2013; Nithyanandam *et al.*, 2011; Xu *et al.*, 2010). A wide range of modifications in any domain could be utilized for watermarking techniques (Junxiao *et al.*, 2011) On the other hand video market is become more and more popular; the cameras' information results have a major role in safety of environment and people. In order not to change the concept of visual information, the embedded data should be

imperceptible and robust. Hence, in addition to robustness and imperceptibility the constraint of computational is imposed to video watermarking (Hasnaoui and Mitrea, 2012).

Video application requires a large quantity of sequences to be processed. Watermarking techniques can also be applied in the frequency domain. In these techniques higher imperceptibility can be obtained as well as better robustness. The disadvantage of frequency domain methods is that they are computationally expensive when compared with spatial. Spatial domain techniques are best suit for video watermarking than other watermarking domains. Watermark can also be embedded in the frequency domains (Chimanna and Khot, 2013). In transform domain, first the host is converted to the frequency domain then the watermark is added and then the inverse frequency transform is applied. One of the common transform methods is the Discrete Cosine Transform (DCT) which divides the image into low, middle and high frequency bands. In the aspect of imperceptibility the middle band is best chosen rather than two other frequency bands. If the watermark is embedded in high frequency band, the details of the edges and other information would be affected. On the other hand, when the watermark is embedded into the low frequency, the imperceptibility is influenced negatively. The DCT is not more efficient than spatial domain when it comes to transparency and also it has intensive computation relatively (Yu *et al.*, 2014). Another common transform method is Discrete Wavelet Transform (DWT) which decompose the image into four sub bands that are low resolution approximation (LL), horizontal (HL), vertical (LH) and diagonal (HH) of detail components. The edge and texture patterns are located in high resolution sub bands. The watermark cannot embed in LL because the smoother part of the image is in this part and also the watermark cannot embed in HH because major details of the image will be lost. That is why the HL and LH are normally selected for watermarking (Chimanna and Khot, 2013; Sinha et al., 2011). The DWT also is not more efficient than spatial domain in aspect of transparency and also have more computation compared to DCT.

## 1.3 Statement of the Problem

The most common approach for concealing information in the video host is spatial domain. The robustness of spatial domain techniques is not as high as other techniques. In order to improve the robustness of spatial domain, a watermark can be embedded several times repeatedly. As a result, if a single copy of that watermark can survive after attacks, that can be retrieved and the techniques passes the robustness test. Moreover, although spatial domain technique is easy to implement, sometimes adding noise entirely demolish the watermark and could be noticeable for attacker by comparing the anticipated sample with the received signal (Agarwal *et al.*, 2012).

In order for spatial domain techniques to be as efficient as other techniques, more payload is needed to embed additional information. The additional information would include the redundant watermarks to ensure the achievable robustness and more metadata of pixels to ensure achievable efficiency to detect more attacks. All these required additional information will degrade the quality (imperceptibility).

## 1.4 Research Questions

During conducting this research we try to find a suitable answer for the following questions:

(i) What are the recent tamper detection techniques for video watermarking in spatial domain?

(ii) How to improve imperceptibility and efficiency of video tamper detection watermarking techniques in spatial domain?

(iii) How efficiency is the proposed technique?

## 1.5 Research Objectives

The exact research targets are as follows:

(i) To study and investigate recent tamper detection techniques for video watermarking in spatial domain

(ii) To propose a video tamper detection watermarking technique in order to improve imperceptibility and efficiency

(iii) To evaluate the efficiency of proposed technique

## 1.6 Scope of the Study

This research has been focused on following scopes;

(i) Digital video watermarking

(ii) Tamper detection on watermarked video

(iii) Vowel less video

(iv) Audio Video Interleave (AVI) files format.

(v) Uncompressed data part of AVI (dB)

(vi) Spatial domain techniques is used

(vii) C # is used for programming

(viii) Avihex is used for visually compare files and check AVI files

(ix) VirtualDub is used for expanding and combining the video frames

(x) Microsoft Windows Paint and Microsoft office picture manager is used for applying attacks

(xi) Efficiency and robustness of nine attacks (Frame Insert, Frame Exchange, Frame Deletion, Crop, Rotate, and Reverse Rotate, Frame shift, Salt and Pepper and Superimpose attack)

## 1.7 Significance of the Study

The more watermarked pixels yield the more detectable pixels. Indeed, the techniques to be more efficient, more payload is needed to embed. The additional information would include the redundant watermarks to ensure the achievable robustness and more metadata of pixels to ensure achievable efficiency to detect more attacks. All these required additional information will degrade the imperceptibility (Agarwal *et al.,* 2012). The watermark should not affect on visual information. Therefore, the output of the research is an appropriate solution for

tamper detection. Furthermore, the vision difference between original video and watermarked video is not recognizable. Additionally the method has high security and is robust against various modifications such as frame cut, frame swapping and frame insertion and variety of geometric attacks (Sinha *et al.*, 2011).

## 1.8 Summary

This chapter focuses on the purpose and the need for this research to be done. Background of the problem, objectives, scope and significance of study is expressed in this chapter. In next chapters all the relevant information is covered as a reference to achieve the objectives of this research.

## REFERENCES


Agarwal, H., Ahuja, R., and Bedi, S. (2012). Highly Robust and Imperceptible Luminance Based Hybrid Digital Video Watermarking Scheme for Ownership Protection. *International Journal of Image, Graphics & Signal Processing.* 4(11).

Al-Haj, A., Mohammad, A., and Bata, L. (2011). DWT-Based Audio Watermarking. *International Arab Journal of Information Technology.* 8(3), 326-333.

Ali, M., and Ahn, C. W. (2014). An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain. *Signal Processing.* 94, 545-556.

Ali, M., Ahn, C. W., and Pant, M. (2014). A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik.* 125(1), 428-434.

Alnawok, F., and Ahmed, B. (2008). Multi-Segment Steganography Technique. *International Arab Journal of Information Technology (IAJIT).* 5(3).

Amira, H., Rhouma, R., and Belghith, S. (2010). An Eigen value based Watermarking scheme for tamper detection in gray level images. *Systems Signals and Devices (SSD), 2010 7th International Multi-Conference on*. 1-5.

Amirgholipour, S., and Sharifi, A. (2014). A Pre-Filtering Method to Improve Watermark Detection Rate in DCT Based Watermarking. *International Arab Journal of Information Technology.* 11(2), 178-185.

Atawneh, S., Almomani, A., and Sumari, P. (2013). Steganography in digital images: Common approaches and tools. *Iete Technical Review.* 30(4), 344-358.

Behnia, S., Teshnehlab, M., and Ayubi, P. (2010). Multiple-watermarking scheme based on improved chaotic maps. *Communications in Nonlinear Science and Numerical Simulation.* 15(9), 2469-2478.

Bhatnagar, G., and Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces.* 31(5), 1002-1013.

Cedillo-Hernandez, A., Cedillo-Hernandez, M., Garcia-Vazquez, M., Nakano-Miyatake, M., Perez-Meana, H., and Ramirez-Acosta, A. (2014). Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT. *Signal Processing.* 97, 40-54.

Cedillo-Hernandez, M., Garcia-Ugalde, F., Nakano-Miyatake, M., and Manuel Perez-Meana, H. (2014). Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification. *Signal Image and Video Processing.* 8(1), 49-63.

Cedillo-Hernandez, M., Garcia-Ugalde, F., Nakano-Miyatake, M., and Perez-Meana, H. (2013). Robust Object-Based Watermarking Using SURF Feature Matching and DFT Domain. *Radioengineering.* 22(4), 1057-1071.

Cetin, O., Akar, F., Ozcerit, A. T., Cakiroglu, M., and Bayilmis, C. (2012). A blind steganography method based on histograms on video files. *Imaging Science Journal.* 60(2), 75-82.

Chaluvadi, S. B., and Prasad, M. V. (2009). Efficient image tamper detection and recovery technique using dual watermark. *Nature & Biologically Inspired Computing, 2009. NaBIC 2009. World Congress on*. 993-998.

Chang, C.-C., Chen, K.-N., Lee, C.-F., and Liu, L.-J. (2011). A secure fragile watermarking scheme based on chaos-and-hamming code. *Journal of Systems and Software.* 84(9), 1462-1470.

Chang, C.-C., Lin, C.-Y., and Fan, Y.-H. (2011). Reversible Steganography for BTC-compressed Images. *Fundamenta Informaticae.* 109(2), 121-134.

Chang, X., Wang, W., Zhao, J., and Zhang, L. (2011). A survey of digital video watermarking. *Natural Computation (ICNC), 2011 Seventh International Conference on*. 61-65.

Cheddad, A., Condell, J., Curran, K., and Mc Kevitt, P. (2009). A skin tone detection algorithm for an adaptive approach to steganography. *Signal Processing.* 89(12), 2465-2478.

Chen, C.-H., Tang, Y.-L., and Hseih, W.-S. (2013). Print-and-Scan Resilient Watermarking through Polarizing DCT Coefficients. *Ieice Transactions on Information and Systems.* E96D(10), 2208-2214.

Chen, H.-y., and Zhu, Y.-s. (2012). A robust watermarking algorithm based on QR factorization and DCT using quantization index modulation technique. *Journal of Zhejiang University-Science C-Computers & Electronics.* 13(8), 573-584.

Chen, S., and Leung, H. (2008). Chaotic watermarking for video authentication in surveillance applications. *Circuits and Systems for Video Technology, IEEE Transactions on.* 18(5), 704-709.

Chen, T.-Y., Istanda, V., Chen, T.-H., Wang, D.-J., and Lin, Y.-L. (2010). H.264 VIDEO AUTHENTICATION BASED ON SEMI-FRAGILE WATERMARKING. *International Journal of Innovative Computing Information and Control.* 6(3B), 1411-1420.

Chimanna, M. A., and Khot, S. (2013). Robustness of video watermarking against various attacks using Wavelet Transform techniques and Principle Component Analysis. *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*. 613-618.

Choi, O., Jeon, I., Yoo, S.-W., and Moon, S. (2013). An Extended DCT Domain Watermarking for Robot Vision against Geometric Image Attacks. *Journal of Applied Mathematics*.

Cichowski, J., Czyzewski, A., and Ieee. (2011). *Reversible Video Stream Anonymization for Video Surveillance Systems Based on Pixels Relocation and Watermarking*.

Coskun, I., Akar, F., and Cetin, O. (2013). A new digital image steganography algorithm based on visible wavelength. *Turkish Journal of Electrical Engineering and Computer Sciences.* 21(2), 548-564.

Cui, D., and Zuo, J. Interest authentication and tamper detection digital watermarking method, involves determining region of interest by user to generate digital watermark and HASH code to trusted third party.

Das, C., Panigrahi, S., Sharma, V. K., and Mahapatra, K. K. (2014). A novel blind robust image watermarking in DCT domain using. inter-block coefficient correlation. *Aeu-International Journal of Electronics and Communications.* 68(3), 244-253.

Do, H., Choi, D., Choi, H., and Kim, T. (2008). Digital video watermarking based on histogram and temporal modulation and robust to camcorder recording.

*Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium on*. 330-335.

Elbasi, E. (2012). Robust MPEG Watermarking in DWT Four Bands. *Journal of Applied Research and Technology.* 10(2), 87-93.

Fallahpour, M., and Megias, D. (2010). DWT-Based High Capacity Audio Watermarking. *Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences.* E93A(1), 331-335.

Fallahpour, M., Shirmohammadi, S., Semsarzadeh, M., and Zhao, J. (2014). Tampering Detection in Compressed Digital Video Using Watermarking. *Ieee Transactions on Instrumentation and Measurement.* 63(5), 1057-1072.

Findik, O., Babaoglu, I., and Ulker, E. (2010). A digital robust image watermarking against desynchronization attacks. *Scientific Research and Essays.* 5(16), 2288-2294.

Golshan, F., and Mohammadi, K. (2013). A hybrid intelligent SVD-based perceptual shaping of a digital image watermark in DCT and DWT domain. *Imaging Science Journal.* 61(1), 35-46.

Guan, Y. L., and Poh, C. L. Method for preparing digital medical image for secure transmission, involves embedding code for tamper detection and localization into digital medical image using reversible watermarking process.

Guan, Z. L. Q. L. S., and Peng, X. (2009). a robust watermarking algorithm based on differential energy and qim for uncompressed video.

Han, S., Chu, C.-H., and Luo, Z. (2011). Tamper Detection in the EPC Network Using Digital Watermarking. *Ieee Security & Privacy.* 9(5), 62-69.

Hasnaoui, M., and Mitrea, M. (2012). Semi-fragile watermarking for video surveillance applications. *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European*. 1782-1786.

He, Y., Yang, G., and Zhu, N. (2012). A real-time dual watermarking algorithm of H.264/AVC video stream for Video-on-Demand service. *Aeu-International Journal of Electronics and Communications.* 66(4), 305-312.

Ishtiaq, M., Jaffar, M. A., Khan, M. A., Jan, Z., and Mirza, A. M. (2009). *Robust and imperceptible watermarking of video streams for low power devices*. In *Signal Processing, Image Processing and Pattern Recognition* (pp. 177-184): Springer.

Jayanthi, V. E., Rajamani, V., and Karthikayen, P. (2011). Performance analysis for geometrical attack on digital image watermarking. *International Journal of Electronics.* 98(11), 1565-1580.

Jin, C., and Pan, M. HTML webpage tamper detection and positioning method, involves producing line of webpage digital watermark, and positioning rows and lines in webpage digital watermark with different authentication codes.

Junxiao, X., Qingbin, L., and Zhiyong, L. (2011). A novel digital video watermarking algorithm. *Procedia Engineering.* 24, 90-94.

Keyvanpour, M., and Bayat, F. M. (2013). Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the DWT domain. *Mathematical and Computer Modelling.* 58(1-2), 56-67.

Kumar, M., and Newman, R. (2010). J3: High payload histogram neutral JPEG steganography. *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*. 46-53.

Kurniawan, M. T., Adiwijaya, Agung, W., and Ieee. (2012). Multiple Watermarking On Digital Medical Images for Tamper Detection and Integrity Control. *2012 2nd International Conference on Uncertainty Reasoning and Knowledge Engineering (Urke)*, 145-148.

Kwitt, R., Meerwald, P., and Uhl, A. (2011). Lightweight Detection of Additive Watermarking in the DWT-Domain. *Ieee Transactions on Image Processing.* 20(2), 474-484.

Lamgunde, A., and Kale, A. (2011). *Palette Based Technique for Image Steganography*. In *Advances in Computing, Communication and Control* (pp. 364-371): Springer.

Lee, M.-J., Im, D.-H., Lee, H.-Y., Kim, K.-S., and Lee, H.-K. (2012). Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues. *Digital Signal Processing.* 22(1), 190-198.

Lei, M., Yang, Y., Luo, S., and Niu, X. (2010). Semi-Fragile Audio Watermarking Algorithm in DWT Domain. *China Communications.* 7(4), 71-75.

Lenarczyk, P., and Piotrowski, Z. (2013). Parallel blind digital image watermarking in spatial and frequency domains. *Telecommunication Systems.* 54(3), 287-303.

Li, C.-T. (2009). Authentication and recovery of digital images: potential application in video surveillance and remote sensing. *2009 Digest of Technical Papers International Conference on Consumer Electronics*. 1-2.

Lin, S. D., Chuang, C.-Y., Chen, M.-J., and Meng, H.-C. (2009). A Novel Video Watermarking Scheme in H. 264/AVC Encoder. *Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on*. 357-360.

Ling, H., Wang, L., and Zou, F. (2011). Real-time video watermarking scheme resistant to geometric distortions. *Journal of Electronic Imaging.* 20(1).

Liu, F., and Wu, C.-K. (2011). Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners. *Information Security, IET*. 5(2), 121-128.

Liu, J., and She, K. (2012). A Hybrid Approach of DWT and DCT for Rational Dither Modulation Watermarking. *Circuits Systems and Signal Processing.* 31(2), 797-811.

Liu, M. (2012). Study of Digital Video Watermarking. *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*. 77-80.

Liu, Z., Li, Q., Guan, S., and Peng, X. (2009). A robust watermarking algorithm based on differential energy and QIM for uncompressed video. *Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on*. 382-385.

Lu, W., Sun, W., and Lu, H. (2009). Robust watermarking based on DWT and nonnegative matrix factorization. *Computers & Electrical Engineering.* 35(1), 183-188.

Lu, W., Sun, W., and Lu, H. (2012). Novel robust image watermarking based on subsampling and DWT. *Multimedia Tools and Applications.* 60(1), 31-46.

Masoumi, M., and Amiri, S. (2013). A blind scene-based watermarking for video copyright protection. *Aeu-International Journal of Electronics and Communications.* 67(6), 528-535.

Masoumi, M., and Amiri, S. (2014). Content Protection in Video Data Based on Robust Digital Watermarking Resistant to Intentional and Unintentional Attacks. *International Arab Journal of Information Technology.* 11(2), 204-212.

Mohanty, S. P., and Kougianos, E. (2011). Real-time perceptual watermarking architectures for video broadcasting. *Journal of Systems and Software.* 84(5), 724-738.

Munoz Munoz, A., and Argueelles Alvarez, I. (2013). COMPUTATIONAL LINGUISTICS AND LINGUISTIC STEGANOGRAPHY. DISTRIBUTING HIDDEN INFORMATION WITH MINIMAL RESOURCES. *Arbor-Ciencia Pensamiento Y Cultura.* 189(760).

Nakamoto, M., Sayama, K., Muneyasu, M., Harano, T., and Ohno, S. (2011). Improvement of Detection Performance in DWT-Based Image Watermarking under Specified False Positive Probability. *Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences.* E94A(2), 661-670.

Nithyanandam, S., Gayathri, K., Raja, K., and Priyadarsini, P. (2011). Recent Trends in Secure Personal Authentication for Iris Recognition Using Novel Cryptographic Algorithmic Techniques. *Process Automation, Control and Computing (PACC), 2011 International Conference on*. 1-6.

Paunwala, M., and Patnaik, S. (2014). Biometric template protection with DCT-based watermarking. *Machine Vision and Applications.* 25(1), 263-275.

Poljicak, A., Mandic, L., and Agic, D. (2011). ROBUSTNESS OF A DFT BASED IMAGE WATERMARKING METHOD AGAINST AM HALFTONING. *Tehnicki Vjesnik-Technical Gazette.* 18(2), 161-166.

Poonkuntran, S., and Rajesh, R. S. (2014). Chaotic model based semi fragile watermarking using integer transforms for digital fundus image authentication. *Multimedia Tools and Applications.* 68(1), 79-93.

Preda, R. O., and Vizireanu, D. N. (2010). A robust digital watermarking scheme for video copyright protection in the wavelet domain. *Measurement.* 43(10), 1720-1726.

Preda, R. O., and Vizireanu, D. N. (2011a). Robust wavelet-based video watermarking scheme for copyright protection using the human visual system. *Journal of Electronic Imaging.* 20(1).

Preda, R. O., and Vizireanu, N. D. (2011b). Quantisation-based video watermarking in the wavelet domain with spatial and temporal redundancy. *International Journal of Electronics.* 98(3), 393-405.

Rahman, S. M. M., Ahmad, M. O., and Swamy, M. N. S. (2009). A New Statistical Detector for DWT-Based Additive Image Watermarking Using the Gauss-Hermite Expansion. *Ieee Transactions on Image Processing.* 18(8), 1782-1796.

Rathore, S. A., Gilani, S., Mumtaz, A., Jameel, T., and Sayyed, A. (2007). Enhancing invisibility and robustness of DWT based video watermarking scheme for copyright protection. *Information and Emerging Technologies, 2007. ICIET 2007. International Conference on.* 1-5.

Reyes, R., Cruz, C., Nakano-Miyatake, M., and Perez-Meana, H. (2010). Digital Video Watermarking in DWT Domain Using Chaotic Mixtures. *Ieee Latin America Transactions.* 8(3), 304-310.

Roy, S. D., Li, X., Shoshan, Y., Fish, A., and Yadid-Pecht, O. (2013). Hardware Implementation of a Digital Watermarking System for Video Authentication. *Ieee Transactions on Circuits and Systems for Video Technology.* 23(2), 300-312.

Saglam, A., Temizel, A., and Ieee. (2009). *Real-time Adaptive Camera Tamper Detection for Video Surveillance.*

Shi, Y., Qi, M., Yi, Y., Zhang, M., and Kong, J. (2013). Object based dual watermarking for video authentication. *Optik.* 124(19), 3827-3834.

Singh, R., Vatsa, M., Singh, S. K., and Upadhyay, S. (2009). Integrating SVM classification with SVD watermarking for intelligent video authentication. *Telecommunication Systems.* 40(1-2), 5-15.

Sinha, S., Bardhan, P., Pramanick, S., Jagatramka, A., Kole, D. K., and Chakraborty, A. (2011). Digital video watermarking using discrete wavelet transform and principal component analysis. *International Journal of Wisdom Based Computing.* 1(2), 7-12.

Sleit, A., Abusharkh, S., Etoom, R., and Khero, Y. (2012). An enhanced semi-blind DWT-SVD-based watermarking technique for digital images. *Imaging Science Journal.* 60(1), 29-38.

Su, P.-C., Lu, M.-T., and Wu, C.-Y. (2013). A practical design of high-volume steganography in digital video files. *Multimedia Tools and Applications.* 66(2), 247-266.

Su, P.-C., Wu, C.-S., Chen, I.-F., Wu, C.-Y., and Wu, Y.-C. (2011). A practical design of digital video watermarking in H.264/AVC for content authentication. *Signal Processing-Image Communication.* 26(8-9), 413-426.

Su, P.-C., Wu, C.-Y., and Chen, Y.-C. (2008). A digital video watermarking scheme for annotating traffic surveillance videos. *Multimedia Signal Processing, 2008 IEEE 10th Workshop on*. 742-747.

Su, Q., Niu, Y., Wang, Q., and Sheng, G. (2013). A blind color image watermarking based on DC component in the spatial domain. *Optik.* 124(23), 6255-6260.

Sun, T., Jiang, X., Lin, Z., Zhou, Y., Lu, H., and Wang, S. (2010). An H.264/AVC Video Watermarking Scheme in VLC Domain for Content Authentication. *China Communications.* 7(6), 30-36.

Surekha, P., and Sumathi, S. (2012). PERFORMANCE COMPARISON OF OPTIMIZATION TECHNIQUES ON ROBUST DIGITAL-IMAGE WATERMARKING, AGAINST ATTACKS. *Applied Artificial Intelligence.* 26(7), 615-644.

Tashk, A., Danyali, H., Alavianmehr, M. A., and Ieee. (2012). *A Modified Dual watermarking Scheme for digital images with Tamper Localization/detection and recovery Capabilities*.

Tickle, A. J., and Kamfwa, D. (2012). Integration of a Digital Watermarking System into a Morphological Scene Change Detector (MSCD) for Tamper Prevention and Detection. *Unmanned/Unattended Sensors and Sensor Networks Ix.* 8540.

Tokar, T., Kanocz, T., and Levicky, D. (2009). Digital watermarking of uncompressed video in spatial domain. *Radioelektronika, 2009. RADIOELEKTRONIKA'09. 19th International Conference*. 319-322.

Tong, X., Liu, Y., Zhang, M., and Chen, Y. (2013). A novel chaos-based fragile watermarking for image tampering detection and self-recovery. *Signal Processing: Image Communication.* 28(3), 301-308.

Ullah, R., Khan, A., and Malik, A. S. (2013). Dual-purpose semi-fragile watermark: Authentication and recovery of digital images. *Computers & Electrical Engineering.* 39(7), 2019-2030.

Van Schyndel, R. (2010). A Hardware-based Surveillance Video Camera Watermark. *Digital Image Computing: Techniques and Applications (DICTA), 2010 International Conference on*. 343-348.

Voloshynovskiy, S., Pereira, S., Iquise, V., and Pun, T. (2001). Attack modelling: towards a second generation watermarking benchmark. *Signal processing.* 81(6), 1177-1214.

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., and Su, J. K. (2001). Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *Communications Magazine, IEEE.* 39(8), 118-126.

Wang, C.-C., and Hsu, Y.-C. (2010). Fragile watermarking scheme for H.264 video authentication. *Optical Engineering.* 49(2).

Wang, J., Healy, R., and Timoney, J. (2011). A robust audio watermarking scheme based on reduced singular value decomposition and distortion removal. *Signal Processing.* 91(8), 1693-1708.

Wang, J., Liu, G., Dai, Y., Sun, J., Wang, Z., and Lian, S. (2008). Locally optimum detection for Barni's multiplicative watermarking in DWT domain. *Signal Processing.* 88(1), 117-130.

Wang, L., Ling, H., Zou, F., and Lu, Z. (2012). Real-Time Compressed-Domain Video Watermarking Resistance to Geometric Distortions. *Ieee Multimedia.* 19(1), 70-79.

Wang, N., and Kim, C.-H. (2009). Color image of tamper detection and recovery using block-based watermarking. *Embedded and Multimedia Computing, 2009. EM-Com 2009. 4th International Conference on*. 1-6.

Wernke, M., Skvortsov, P., Dürr, F., and Rothermel, K. (2014). A classification of location privacy attacks and approaches. *Personal and Ubiquitous Computing.* 18(1), 163-175.

Wu, Z.-Y., Tseng, Y.-J., Chung, Y., Chen, Y.-C., and Lai, F. (2012). A Reliable User Authentication and Key Agreement Scheme for Web-Based Hospital-Acquired Infection Surveillance Information System. *Journal of Medical Systems.* 36(4), 2547-2555.

Xu, D., Wang, R., and Wang, J. (2011). A novel watermarking scheme for H.264/AVC video authentication. *Signal Processing-Image Communication.* 26(6), 267-279.

Xu, D., Zhang, J., and Pang, B. (2010). A Digital Watermarking Scheme Used for Authentication of Surveillance Video. *Computational Intelligence and Security (CIS), 2010 International Conference on*. 654-658.

Xuemei, J., Quan, L., and Qiaoyan, W. (2013). A new video watermarking algorithm based on shot segmentation and block classification. *Multimedia tools and applications.* 62(3), 545-560.

Yesilyurt, M., Yalman, Y., and Ozcerit, A. T. (2013). A New DCT Based Watermarking Method Using Luminance Component. *Elektronika Ir Elektrotechnika.* 19(4), 47-52.

Yu, P. F., Yu, P. C., and Xu, D. (2014). Palmprint Authentication Based on DCT-Based Watermarking. *Applied Mechanics and Materials.* 457, 893-898.

Zhang, Q., Chen, C., Wei, X., and Ma, R. (2011). A Robust Digital Image Watermarking Method Against Geometric Attacks. *Information-an International Interdisciplinary Journal.* 14(10), 3537-3547.

Zhang, Y. (2009). Digital Watermarking Technology: A Review. *Future Computer and Communication, 2009. FCC'09. International Conference on*. 250-252.

Zhao, H., Wang, F., Chen, Z., and Liu, J. (2014). A Robust Audio Watermarking Algorithm Based on SVD-DWT. *Elektronika Ir Elektrotechnika.* 20(1), 75-80.

Zheng, J., Feng, S., and Zhang, Y. (2009). A Color Image Watermarking Scheme in the Associated Domain of DWT and DFT Domains Based on Multi-channel Watermarking Framework. *Chinese Journal of Electronics.* 18(4), 665-670.